

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-223689

(43)Date of publication of application : 17.08.2001

(51)Int.Cl. H04L 9/20
H04Q 7/38(21)Application number : 2000-376109 (71)Applicant : HYNIX SEMICONDUCTOR
INC

(22)Date of filing : 11.12.2000 (72)Inventor : BOKU SEICHIN

(30)Priority

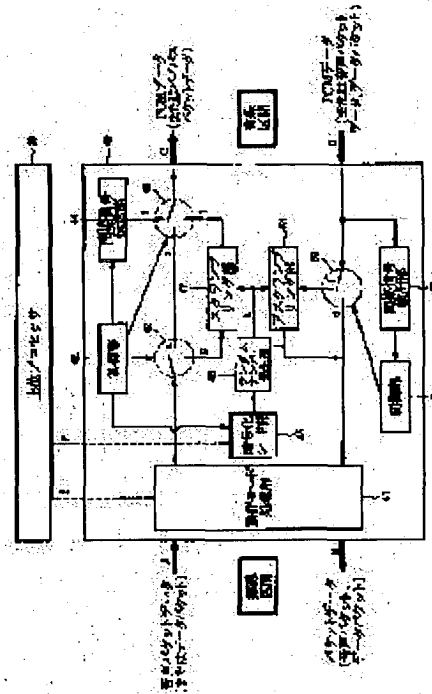
Priority number : 1999 9958711 Priority date : 17.12.1999 Priority country : KR

(54) VOICE AND DATA ENCRYPTION/DECODING UNIT FOR MOBILE
COMMUNICATION SYSTEM AND ITS METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a voice and data encryption/decoding unit in a mobile communication system, that can prevent wire tapping and to provide its method.

SOLUTION: The unit for encrypting/decoding voice/data and its method in a mobile communication system subjects VOCODing or bypassing a signal sent from a wireless channel block to scramble the VOCODing and bypassed signal, through the use of a random number and transmit the scrambled signal to a wired channel block. Furthermore, the scrambled signal received from the wired channel block is descrambled according to the random number, depending on the presence of detection of a synchronizing signal, vocoded or bypassed and sent to the wireless channel block. Thus, maintainability in the wired channel block between the system and the vocoder can be maintained considerably, so as to prevent wire tapping in advance.



LEGAL STATUS

[Date of request for examination] 11.12.2000

[Date of sending the examiner's
decision of rejection][Kind of final disposal of application
other than the examiner's decision of
rejection or application converted
registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-223689

(P2001-223689A)

(43) 公開日 平成13年8月17日 (2001.8.17)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 L 9/20		H 0 4 L 9/00	6 5 3
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R

審査請求 有 請求項の数12 O L (全 10 頁)

(21) 出願番号 特願2000-376109(P2000-376109)

(22) 出願日 平成12年12月11日 (2000. 12. 11)

(31) 優先権主張番号 1 9 9 9 - 5 8 7 1 1

(32) 優先日 平成11年12月17日 (1999. 12. 17)

(33) 優先権主張国 韓国 (K R)

(71) 出願人 591024111

株式会社ハイニックスセミコンダクター

大韓民国京畿道利川市夫鉢邑牙美里山136-1

(72) 発明者 朴 正 鎮

大韓民国京畿道利川市夫鉢邑牙美里山136-1

(74) 代理人 100057874

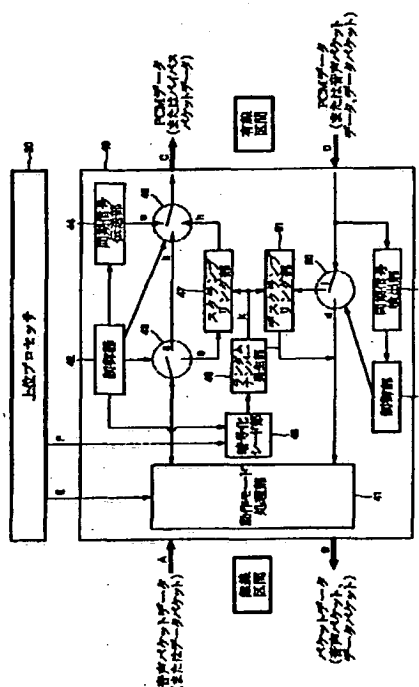
弁理士 曾我 道照 (外6名)

(54) 【発明の名称】 移動通信システムの音声及びデータ暗号化/復号化装置及びその方法

(57) 【要約】

【課題】 盗聴を防止できるようにした移動通信システムにおける音声及びデータ暗号化/復号化装置及びその方法を提供する。

【解決手段】 本発明による移動通信システムの音声/データを暗号化/復号化するための装置及びその方法は、無線チャネル区間から伝送されてきた信号をボコーディングまたはバイパスさせた後、ボコーディングまたはバイパスされた信号をランダムナンバーを利用してスクランプリングして有線チャネル区間に伝送する。また、有線チャネル区間から受信されるスクランプリングされた信号を同期信号の検出有無によりランダムナンバーでデスクランプリングした後、ボコーディングまたはバイパスさせて無線チャネル区間に伝送する。こうようにすることで、システムボコード間、有線チャネル区間における保安性を画期的に維持させ盗聴を未然に防止できる。



【特許請求の範囲】

【請求項1】 移動通信システムの音声／データボコーディング装置において、

音声及びデータの動作モードを制御する動作モード制御信号、データ暗号化のための暗号化キー供給制御信号、同期信号発生制御信号を生じる制御部と、前記制御部から発生した動作モード制御信号により無線チャンネル区間から伝送されてきた音声／データパケットをボコーディングしたりバイパスさせる動作モード処理部と、

前記制御部から発生した暗号化キー供給制御信号によりランダムナンバーを発生させるランダムナンバー発生部と、

前記制御部から発生した同期信号発生制御信号により同期信号を生じて有線チャンネル区間に伝送する同期信号伝送部と、

前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたPCMまたは音声／データパケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャンネル区間に伝送する暗号化部とを含んで構成されたことを特徴とする移動通信システムの音声及びデータ暗号化装置。

【請求項2】 前記制御部の制御信号により同期信号発生部にスイッチングされて発生した同期信号を有線チャンネル区間に伝送した後、同期信号の伝送が完了すると提供される制御信号により前記暗号化部にスイッチングされて暗号化された信号を有線チャンネル区間に伝送するスイッチング部をさらに備えることを特徴とする請求項1記載の移動通信システムの音声及びデータ暗号化装置。

【請求項3】 前記制御部の制御信号により貯蔵された暗号化キーを前記ランダムナンバー発生部に供給する暗号化キー供給部をさらに備えることを特徴とする請求項1記載の移動通信システムの音声及びデータ暗号化装置。

【請求項4】 前記ランダムナンバー発生部から発生したランダムナンバーは、前記動作モード処理部でボコーディングされたPCMまたはバイパスされた音声／データパケットデータを暗号化するための任意の位置情報であることを特徴とする請求項1記載の移動通信システムの音声／データ暗号化装置。

【請求項5】 移動通信システムの音声及びデータボコーディング装置において、有線チャンネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、前記同期信号検出部で同期信号が検出されると、前記復号化制御信号及び動作モード制御信号を提供して、復号化キーを供給できるように制御信号を提供する制御部と、前記制御部から提供される復号化キーによりランダムナ

ンバーを生じるランダムナンバー発生部と、

前記制御部から提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーで有線チャンネルから受信された暗号化された信号を復号化する復号化部と、

前記制御部から提供される動作モードにより前記復号化部で復号化されたPCMをボコーディングしてパケットに変換したりまたは音声／データパケットをそのままバイパスさせた後、無線チャンネル区間に伝送する動作モード処理部とを含んで構成されたことを特徴とする移動通信システムの音声／データ復号化装置。

【請求項6】 前記制御部から提供される制御信号により有線チャンネルから伝送されてきた暗号化された信号を前記復号化部にスイッチングするスイッチング部をさらに備えることを特徴とする請求項5記載の移動通信システムの音声及びデータ復号化装置。

【請求項7】 前記制御部の制御信号により貯蔵された暗号化キーを前記ランダムナンバー発生部に供給する復号化キー供給部をさらに備えることを特徴とする請求項5記載の移動通信システムの音声及びデータ暗号化方法。

【請求項8】 前記ランダムナンバー発生部から発生したランダムナンバーは、前記有線チャンネル区間から受信したPCMまたは音声／データパケットデータを復号化するための任意の位置情報であることを特徴とする請求項5記載の移動通信システムの音声／データ暗号化装置。

【請求項9】 移動通信システムの音声／データボコーディング装置において、無線チャンネル区間から伝送されてきた音声／データパケットを提供される動作モード信号によりボコーディングしたりバイパスさせて、復号化されたPCMまたはパケットを提供される動作モードによりボコーディングまたはバイパスさせて無線チャンネル区間に伝送する動作モード処理部と、

供給される暗号化及び復号化キーによりランダムナンバーを発生させるランダムナンバー発生部と、

提供される制御信号により同期信号を生じて有線チャンネル区間に伝送する同期信号伝送部と、

前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたPCMまたは音声／データパケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャンネル区間に伝送する暗号化部と、

有線チャンネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、

提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーにより有線チャンネルから受信された暗号化された信号を復号化する復号化部と、

前記同期信号検出部で同期信号が検出されると、前記復号化部に復号化制御信号を提供して、前記暗号化キー及び復号化キーを供給できるように制御信号を提供して、前記同期信号発生制御信号を提供する制御部とで構成されたことを特徴とする移動通信システムの音声及びデータ暗号化／復号化装置。

【請求項10】 前記制御部の制御信号により貯蔵された暗号化キー及び復号化キーを前記ランダムナンバー発生部に供給する復号化キー供給部をさらに備えることを特徴とする請求項9記載の移動通信システムの音声及びデータ暗号化／復号化方法。

【請求項11】 移動通信システムの音声及びデータボコーディング方法において、無線チャネル区間から伝送されてきた音声パケットまたはデータパケットを提供される動作モードによりボコーディングまたはバイパスさせた後出力する段階と、暗号化キー情報により任意の一定なランダムナンバーを生じる段階と、

同期信号を生成してその生成した同期信号を有線チャネル区間に伝送する段階と、

前記同期信号が伝送されると前記発生したランダムナンバーを利用して前記モード処理された信号（PCMまたはバイパスされた音声パケットまたはバイパスされたデータパケット）を暗号化した後、暗号化された信号を有線チャネル区間に伝送する段階とで構成されることを特徴とする移動通信システムの音声及びデータ暗号化方法。

【請求項12】 移動通信システムの音声及びデータボコーディング方法において、有線チャネル区間から暗号化された信号を受信する段階と、

暗号化された信号が受信されると、その暗号化された信号から同期信号を検出する段階と、

前記同期信号が検出されると、復号化キーにより任意の一定なランダムナンバーを生じる段階と、

前記発生したランダムナンバーにより前記暗号化された信号を復号化する段階と、

前記復号化されたPCMまたはパケットを動作モードによりボコーディングまたはバイパスさせてパケットに変換した後、無線チャネル区間に伝送する段階とで構成されることを特徴とする移動通信システムにおける音声及びデータ復号化方法。

【発明の詳細な説明】

【0001】、

【発明の属する技術分野】本発明は、移動通信システムの音声及びデータボコーディングに関するもので、特に、デジタル移動通信システムのボコーディング装置で移動加入者間音声通話及びデータ通信時システム内ボコードの動作モードに関係なく有線チャネル上の通信信号を暗号化及び復号化するための移動通信システムにおけ

る音声及びデータ暗号化／復号化装置及びその方法に関するものである。

【0002】

【従来の技術】一般に、デジタル移動通信システムで制限された無線チャネル容量内に多数の加入者を受容するために音声圧縮して伝送する。音声圧縮するためには音声符号化アルゴリズムを使用しなければならないが、一般に移動通信分野では低伝送率でありながら有線網音質を有するボコーディング（Vocoding）アルゴリズムを用いる。ボコーディングアルゴリズムは、誤差があるアルゴリズムであるので圧縮と復元とを繰り返せばするほど復元された音声と原音声との間の誤差は大きくなる。すなわち、復元された音声の音質が低下する。

【0003】図1は、一般的な移動通信システムにおける移動加入者間の通話時、区間別伝送形態を示した図面である。図示されるように、移動加入者間の通話である時、移動局1、1'で音声圧縮してパケット形態で伝送局2、2'に伝送すると、伝送局システム内のボコード（図示せず）で伝送されたパケットをPCM（Pulse Code Modulation）形態に復元する。この復元されたPCMデータは交換局3を経て通話しようとする相手側移動局1'、1がサービスを受けている伝送局2'、2に送られて、再び伝送局2'、2内にあるボコードで再圧縮をする。ここで、前記伝送局2、2'は制御局と基地局とを含む。このように圧縮されたパケットは、無線チャネルを通して移動局1'、1に伝送される。

【0004】次に、パケットを受信した移動局1、1'は、移動局1、1'内のボコードでパケットを復元することになり、これにより、移動加入者は相手方の音声聞くことができる。結局、移動加入者間の通話時には、2回のボコーディング過程を経るようになることが分かる。そして、移動加入者間の通話である場合、移動局1、1'で圧縮されて無線チャネルに伝送されてきた音声パケットをシステム内にあるボコードでパケットバイパス（Packet Bypass）させることにより、ボコーディング過程を減らすようになり、結局、音質低下を補完できる。また、パケットバイパス機能は、データ通信時にも用いられる。ここで、移動局1、1'と伝送局2、2'の間は無線チャネル区間であり、伝送局2、2'と交換局3との間是有線チャネル区間である。

【0005】以下、図2を参照して従来技術による音声信号のボコーディング装置に対して説明すると次の通りである。図2は、一般的な移動通信システムにおけるボコードバイパスされたパケット類型を示した図面であり、図2（a）はバイパスされた音声パケットのフォーマットを示した図面であり、図2（b）はバイパスされたデータパケットのフォーマットを示した図面であり、

図3は従来技術による移動通信システムにおける動作モード別ボコーディング装置のブロック構成を示した図面である。

【0006】まず、移動通信システムにおけるボコーディング装置は、ボコーダ20と、上位プロセッサ10とで構成される。ここで、上位プロセッサ10は、伝送路2、2'と交換局3全体でボコーダ20を除いた残り部分を総括する部分である。そして、前記ボコーダ20は、第1、2、3、4モードスイッチング部22、26、27、31と、各モード別にボコーディング処理する第1ないし第6ボコーディング処理部23、24、25、28、29、30とで構成される。

【0007】このような構成を有する従来技術による移動通信システムのボコーディング装置は、移動加入者間通話時3種類のモードで動作する。1番目のモードは、通話しようとする移動加入者端末機内のボコーダが異なる種類のボコーダの場合、例えば、EVCR (Enhanced Variable Code Rate) と QCELP (Qualcomm Code Excited Linear Predictive) 間、8Kbps QCELPと13Kbps QCELP間である時であり、システムのボコーダは、正常なボコーディング（音声符号化と復号化）過程を遂行する。この時、無線チャネル（端末機とシステムボコーダとの間の伝送路）上ではパケット形態で通信され、有線チャネル（交換局を間に置いたシステムボコーダ間伝送路）上の伝送形態はPCMである。

【0008】2番目のモードは、通話しようとする移動加入者端末機のボコーダが相互に同一な場合であり、例えば、EVCRとEVCRまたはQCELPとQCELPの時であり、システムのボコーダは、音声パケットバイパス (Voice Packet Bypass) モードで動作する。この時は、無線チャネル上でパケット形態で取り交わし、有線チャネル上における伝送形態は、図2(a)に示されたようなバイパスされた音声パケットである。

【0009】そして、三番目のモードは、移動加入者間データ通信をする場合であり、システムボコーダは、データパケットバイパス (Data Packet Bypass) モードで動作する。この時、無線チャネル区間はパケット形態で取り交わし、有線チャネル区間は図2(b)のようなバイパスされたデータパケット形態で伝送する。

【0010】このように前記した3種類のモードで動作を遂行する従来ボコーディングシステムは図3に示された通りである。図3に示したように、ボコーダ20は、上位プロセッサ10から3種類のモード中、一種類のモードで動作できるモード情報Eを受けてモード制御器21で各モードに合う動作を制御する。すなわち、上位プロセッサ10から前記1番目のモード情報が入力される

と、モード制御器7は、スイッチング部22、26を第1ボコーディング処理部23にスイッチングして移動端末機から無線チャネルAを通して伝送されてきた音声パケットをPCMにボコーディングしてPCMデータを交換局に有線チャネルCを通して伝送する。

【0011】また、モード制御器21は、スイッチング部27、31を第4ボコーディング処理部28にスイッチングさせて交換局から有線チャネルDを通して伝送したPCMデータをパケットデータにボコーディングして無線チャネルBを通して通話しようとする移動端末機に伝送することになる。

【0012】一方、上位プロセッサ10から前記二番目のモード情報が入力されると、モード制御器7は、スイッチング部22、26を第2ボコーディング処理部24にスイッチングして移動端末機から無線チャネルAを通して伝送した音声パケットをバイパスさせて、そのバイパスされた音声パケットデータを有線チャネルCを通して交換局に伝送する。

【0013】また、モード制御器21は、スイッチング部27、31を第5ボコーディング処理部29にスイッチングして交換局から有線チャネルDを通して伝送された音声パケットデータをバイパスさせてバイパスされた音声パケットデータを無線チャネルBを通して通話しようとする移動端末機に伝送することになる。

【0014】また、上位プロセッサ10から前記三番目のモード情報が入力されると、モード制御器7は、スイッチング部22、26を第3ボコーディング処理部23にスイッチングして移動端末機から無線チャネルAを通して伝送されたデータパケットをバイパスさせてバイパスされたデータパケットを交換局に有線チャネルCを通して伝送するようにする。

【0015】また、モード制御器21は、スイッチング部27、31を第6ボコーディング処理部30にスイッチングして交換局から有線チャネルDを通して伝送したデータパケットをバイパスさせてバイパスされたデータパケットを無線チャネルBを通して通話しようとする移動端末機に伝送する。

【0016】前記のように、ボコーダ20は、上位プロセッサ10とモード情報のみならず無線チャネルA、B上を通信するパケットを取り交わし、モード情報により適切な処理過程を遂行し、有線チャネルC、D区間ではモードにより図2に示された形態のようなバイパスされたパケット及びPCMなどを入出力する。

【0017】そして、上位プロセッサ10は、ボコーダ20を制御する役割だけでなく無線チャネルを通して移動局とシステムボコーダ間のパケット通信をするようにする。

【0018】

【発明が解決しようとする課題】このような従来技術によるボコーディングシステムにおいて、システムボコー

ダが前記各モードで動作する時、特に有線チャンネル上で盗聴が容易にできる問題点がある。すなわち、前記第1番目のモードで動作する場合（ボコーディングモードで動作する場合）、有線チャンネル区間で伝送されるPCMは、盗聴装置により容易に盗聴できる。

【0019】そして、2番目のモード、すなわち、音声バケットバイパスモードで動作する場合は、一般のPCM盗聴方法では盗聴できないが、図2(a)で示したように、純粹音声バケットが予め定義されたフィールドに定まった順序通りに位置しているためにバイパスされた音声バケット全体から音声バケットを探することができる位置に対する場合の数は非常に制限的であるため、容易に盗聴されることがある。

【0020】また、前記と類似した3番目のモード、すなわち、データバケットバイパスモードでも、図2

(b)に示されたようにバイパスされたデータバケットが有線チャンネル上で繰り返して表れることになり、同一のパターンを有するフラグフィールド(Flag Field)を除去してしまえば、容易に純粹データバケットを抽出することができるので、盗聴が容易な短所がある。

【0021】本発明は前記のような問題点を解決するために提案されたもので、本発明の目的は、伝送側システムボコダ内に暗号化機能を置いて有線チャンネル上に伝送しようとする通信信号を暗号化して伝送し、受信側システムボコダ内には暗号化されたデータを復号化することができる解読機能を置いて通信信号を解読できるようにして盗聴を防止できるようにした移動通信システムにおける音声及びデータ暗号化復号化装置を提供することにある。また、本発明の他の目的は、前記ボコーディング装置の動作と相応する音声及びデータ暗号化/復号化方法を提供することにある。さらに詳細には、有線チャンネル区間で音声盗聴及びデータの流出を防ぐため保安性を高める必要があり、このためにシステムボコダ内に暗号化器と解読器とをすべて設けて上位プロセッサから提供される同一の暗号化キーを利用して通信信号を暗号化して受信される暗号化された通信信号を解読できるようにした移動通信システムにおける音声及びデータ暗号化/復号化装置及びその方法を提供することにある。

【0022】

【課題を解決するための手段】前記のような目的を達成するための本発明による移動通信システムにおける音声及びデータ暗号化装置の特徴は、音声及びデータの動作モードを制御する動作モード制御信号、データ暗号化のための暗号化キー供給制御信号及び同期信号発生制御信号を生じる制御部と、前記制御部から発生した動作モード制御信号により無線チャンネル区間から伝送されてきた音声/データバケットをボコーディングしたりバイパスさせる動作モード処理部と、前記制御部から発生した暗号化キー供給制御信号によりランダムナンバーを発生さ

せるランダムナンバー発生部と、前記制御部から発生した同期信号発生制御信号により同期信号を生じて有線チャンネル区間に伝送する同期信号伝送部と、前記ランダムナンバー発生部から発生したランダムナンバーを利用して前記動作モード処理部でボコーディングまたはバイパスされたPCMまたは音声/データバケットを暗号化した後、前記同期信号の伝送が完了すると、有線チャンネル区間に伝送する暗号化部とで構成される。

【0023】また、本発明による移動通信システムで音声及びデータ復号化装置の特徴は、有線チャンネル区間から伝送されてきた暗号化された信号から同期信号を検出する同期信号検出部と、前記同期信号検出部から同期信号が検出されると、前記復号化制御信号及び動作モード制御信号を提供して、復号化キーを供給できるように制御信号を提供する制御部と、前記制御部から提供される復号化キーによりランダムナンバーを生じるランダムナンバー発生部と、前記制御部から提供される復号化制御信号により前記ランダムナンバー発生部から発生したランダムナンバーで有線チャンネルから受信された暗号化された信号を復号化する復号化部と、前記制御部から提供される動作モードにより前記復号化部で復号化されたPCMをボコーディングしてバケットに変換したりまたは音声/データバケットをそのままバイパスさせた後、無線チャンネル区間に伝送する動作モード処理部とで構成される。

【0024】また、本発明による移動通信システムにおける音声及びデータ暗号化方法の特徴は、無線チャンネル区間から伝送されてきた音声バケットまたはデータバケットを提供される動作モードによりボコーディングまたはバイパスさせた後出力する段階と、暗号化キー情報により任意の一定なランダムナンバーを生じる段階と、同期信号を生成してその生成した同期信号を有線チャンネル区間に伝送する段階と、前記同期信号が伝送されると前記発生したランダムナンバーを利用して前記モード処理された信号（PCMまたはバイパスされた音声バケットまたはバイパスされたデータバケット）を暗号化した後、暗号化された信号を有線チャンネル区間に伝送する段階とで構成される。

【0025】また、本発明による移動通信システムで音声及びデータ復号化方法の特徴は、有線チャンネル区間から暗号化された信号を受信する段階と、暗号化された信号が受信されると、その暗号化された信号から同期信号を検出する段階と、前記同期信号が検出されると、復号化キーにより任意の一定なランダムナンバーを生じる段階と、前記発生したランダムナンバーにより前記暗号化された信号を復号化する段階と、前記復号化されたPCMまたはバケットを動作モードによりボコーディングまたはバイパスさせてバケットに変換した後、無線チャンネル区間に伝送する段階とで構成される。

【0026】

【発明の実施の形態】以下、本発明による移動通信システムにおける音声及びデータ暗号化／復号化装置及びその方法に対して添付した図面を参照して詳細に説明すると次の通りである。まず、本発明は、前記従来技術で説明したように移動加入者間通話時ボコーダの動作モードにより有線チャンネル区間で伝送される通信信号の類型はすべて3種類である。すなわち、音声通話時ボコーダがボコーディングモードで動作する場合PCMであり、音声パケットバイパスモードで動作する場合にはバイパスされた音声パケットである。そして、データ通信時に、ボコーダはデータパケットバイパスモードで動作し、有線チャンネル区間ではバイパスされたデータパケット形態である。本発明は前記のようなあらゆる類型に対して暗号化及び復号化が可能にする。

【0027】図4は、本発明による移動通信システムにおける音声／データを暗号化して解読するボコーディングシステムのブロック構成を示した図面である。図示されるように、動作モード情報及び暗号化キー情報を提供する上位プロセッサ30と、上位プロセッサ30から提供されるモード情報により入力される端末機で無線チャンネルAを通して伝送した音声またはデータパケットをボコーディングまたはバイパスモードで動作処理して、デスクランプリングされた信号をパケットにボコーディングしたりまたはバイパスモードで動作処理してパケットを無線チャンネルBを通して移動端末機に伝送する動作モード処理部41と、上位プロセッサ30で提供する暗号化キー情報を貯蔵及び貯蔵された暗号化キー情報を出力させるための制御信号、同期信号伝送制御信号及びスイッチング制御信号を各々発生して提供する制御部42と、制御部42から提供される貯蔵制御信号により上位プロセッサ30から提供される暗号化キー情報を貯蔵して、出力制御信号により貯蔵された暗号化キー情報を出力する暗号化キーシード(Seed)部45で構成される。

【0028】また、制御部42から提供される制御信号により一般モードまたは暗号化モードにスイッチング転換する第1スイッチング部43と、暗号化キーシード部45から提供される暗号化キー情報によりランダムナンバー(Random Number)を発生させるランダムナンバー発生部46と、ランダムナンバー発生部46から発生したランダムナンバーにより動作モード処理部41を通してモード処理(ボコーディングまたはバイパス)されたパケットまたはPCM信号を暗号化(Scrambling)するスクランプリング部47と、制御部42から提供される同期信号伝送制御信号により同期信号を発生して、発生された同期信号を伝送する同期信号伝送部44と、前記同期信号伝送部44から伝送された同期信号を先に伝送して、スクランプリング部47出力端にスイッチングしてスクランプリング部47でスクランブルされた信号をスイッチングして暗号化された

データを有線チャンネルCを通して交換局に伝送する第2スイッチング部48とで構成される。

【0029】また、有線チャンネルDを通して受信される暗号化された信号から同期信号を検出する同期信号検出部49と、同期信号検出部49から同期信号が検出されると、制御部42の制御信号により一般モードから解読モードにスイッチング転換する第3スイッチング部50と、第3スイッチング部50のスイッチングにより受信された暗号化された信号を解読(Decrambling)した後、前記動作モード処理部41に出力するデスクランプリング部51とで構成される。

【0030】このような構成を有する本発明による移動通信システムにおける音声／データ暗号化／復号化装置の詳細動作を説明すると次の通りである。まず、ボコーダ40は、上位プロセッサ30から動作モードE及び暗号化キー情報Fを受ける。そうすれば、ボコーダ40の動作モード処理部41及び制御部42で制御信号を生成する。

【0031】すなわち、制御部42は、暗号化キーを暗号化シード部45に貯蔵させた後、貯蔵された暗号化キーをリードしてランダムナンバー発生部46に出力させる。この時、制御部42は第1スイッチング部43をa端からg端にスイッチング転換させるようになる。

【0032】そして、ランダムナンバー発生部46は、暗号化シード部45から提供される暗号化キーにより任意のランダムナンバーを生じてスクランプリング部47に提供する。

【0033】したがって、スクランプリング部47は、第1スイッチング部43のスイッチング転換により動作モード処理部41から出力されるバイパスされたパケットまたはボコーディングされたPCM信号をランダムナンバー発生部46から提供されるランダムナンバーによりスクランブル、すなわち、暗号化させた後、第2スイッチング部48に出力する。

【0034】この時、制御部42は、同期信号伝送部44に制御信号を提供すると同時に第2スイッチング部48にスイッチング制御信号を提供して同期信号伝送部44で発生した同期信号を有線チャンネル区間に先に伝送する。同期信号が伝送されると、制御部42は、第2スイッチング部48をスクランプリング部47にスイッチング転換させて、スクランプリング部47で暗号化された信号を有線チャンネル区間に伝送するようになる。

【0035】ここで、同期信号は、最初のフレームに対する暗号化された信号を有線チャンネル区間に伝送する前に1回のみ伝送するようになり、その後のあらゆるフレームに対しては同期信号を伝送しなくなる。

【0036】一方、有線チャンネル区間で前記のように暗号化されたデータが受信されると、ボコーダ40の同期信号検出部49では受信された暗号化された信号から同期信号を検出して同期信号検出結果を制御部42に提供

する。この時、制御部42は、同期信号検出部49から同期信号が検出されると、第3スイッチング部50をd端からi端にスイッチング転換させる。

【0037】したがって、受信された暗号化された信号、すなわち、スクランプリングされた信号はスクランプリングの逆過程、すなわち、ランダムナンバー発生部46から出力されるランダムナンバーにより解読される。このように解読されたパケットまたはPCM信号は動作モード処理部41に提供される。

【0038】動作モード処理部41は、上位プロセッサ30から提供される動作モードによりボコーディングまたはバイパス動作を遂行してバイパスされたパケットまたはボコーディングされたPCMを無線チャネル区間に伝送するようになる。

【0039】前記暗号化及び復号化機能に対してさらに詳細に説明すると次の通りである。ボコード40は、上位プロセッサ30から動作モード及び暗号化キー情報を受ける。ボコード40は、この情報で動作モード処理部41及び制御部42で制御信号を作る。すなわち、制御部42は、暗号キーを暗号化シード部45に貯蔵させた後、貯蔵された暗号化キーをランダムナンバー発生部46に出力させる。

【0040】これにより、ランダムナンバー発生部46は、暗号化シード部45から提供される暗号化キーによりランダムナンバーを発生させる。この時、ランダムナ

ンバーは、ボコード40の入出力通信信号を暗号化したリ解読する情報として用いられる。この情報は、ボコード40の入出力通信信号の位置情報に該当し、暗号化を遂行するスクランプリング部47と解読を遂行するデスクランプリング部51とに各々入力される。

【0041】スクランプリング部47は、ランダムナンバー発生部46から発生した位置情報を利用して動作モード処理部41から出力された通信信号gの各位置をビットまたはバイト単位で再配列する。この時、暗号化の程度は暗号化しようとする通信信号をバイト単位で再配列することよりはビット単位で再配列することがさらに性能が優れる。このように、再配列された信号hをスクランプリング部47は同期信号伝送部44から発生した同期信号と合成してボコード40出力端Cに出力することにより、暗号化された信号が有線チャネル上に伝送される。

【0042】そして、デスクランプリング部51は、有線チャネル区間から伝送されてきた暗号化された信号Dをランダムナンバー発生部46から発生した位置情報を利用して下記表1のスクランプリング過程の逆過程で信号を逆配列することにより、元来の信号jを解読する。この過程に対する例を下の表1を参考にして説明すると次の通りである。

【0043】

【表1】

原位置	0	1	2	3	4	5	6	7	8	9
通信信号	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9
ランダムナンバー	1	3	5	7	2	9	8	4	6	0
再配列信号	X1	X3	X5	X7	X2	X9	X8	X4	X6	X0

【0044】説明の便宜上、10バイト単位で通信信号gを再配列（暗号化）しようとするならば、0-9間の10個のランダムナンバーkを発生させる。前記の表1のように任意のランダムナンバーが発生したならば、第1番目のランダムナンバーが1であるために1の位置にある通信信号X1を第1番目の位置（位置0）にもってくる。そして、二番目のランダムナンバーが3であるために3の位置にあった通信信号X3を二番目位置（位置1）にもってくる。こういう方法で最後の九番目ランダムナンバーは0であるために0の位置にある通信信号X0を位置（位置9）に移動させる。結局、このようにすれば、一番下の再配列された信号が得られるようになり、これが暗号化された信号になる。解読過程（デスクランプリング）は、前記暗号化過程を逆に遂行すれば、容易に元来の通信信号を逆配列できることが分かる。

【0045】ところで、システムの伝送側と受信側との各ボコードが暗号化された信号を正確に解読するために

は暗号化及び解読を始める時点が一致しなければならない。すなわち、システムボコード間無線チャネル区間で通信信号の伝送遅延に対して考慮しなければならない。これを解決する方法としていろんな方法が有り得るが、システムの設計及び形状により変わる場合がある。ここではいかなるシステムの構造でも動作できる方法として、スクランプリング部47及びデスクランプリング部51が動作する時点に対する同期情報をスクランプリング部47で暗号化された信号を伝送する前に同期信号伝送部44から第2スイッチング部48を通して有線チャネルを通して伝送する。

【0046】また、これと並行して有線チャネルDから受信される同期情報を先に検出した後、同期情報が検出されると受信された暗号化された信号をデスクランプリング部51で前記したような解読方法により解読する。

【0047】したがって、有線チャネル上で伝送側ボコードと受信側ボコードとの間の通信信号伝送遅延で生じ

るスクランプリング部47とデスクランプリング部51との駆動時点に対する不一致を解決することができ、同一暗号キーを利用した通信信号の暗号化及び暗号化された信号の解読機能を正確に遂行できるようになる。この時、前記同期情報は予め約束された一定パターンで構成される。

【0048】以下、添付された図5及び図6を参照して本発明による移動通信システムの音声／データ暗号化方法及び復号化方法を各々区分して段階的に説明すると次の通りである。まず、図5を参照して移動通信システムで音声／データ暗号化方法に対して説明すると次の通りである。まず、無線チャネル区間から伝送されてきた音声パケットまたはデータパケットを上位プロセッサ30から提供される動作モードにより該モードを遂行する

(S101)。すなわち、受信される音声パケットを提供される動作モードによりボコーディングしてPCMに変換したり、音声パケットをバイパスさせたり、またはデータパケットをバイパスさせる。

【0049】次に、上位プロセッサ30から提供される暗号化キー情報により任意の一定なランダムナンバーを生じる(S102)。同時に提供される制御信号により同期信号を生じて、その発生した同期信号を有線チャネル区間に伝送した後(S103)、同期信号の伝送が完了すると前記発生したランダムナンバーを利用して前記モード処理された信号(PCMまたはバイパスされた音声パケットまたはバイパスされたデータパケット)を暗号化する(S104)。このように暗号化された信号を有線チャネル区間に伝送する(S105)。

【0050】そして、図6を参照して有線チャネル区間から伝送されてきた暗号化された信号を解読する方法に対して段階的に説明すると次の通りである。まず、有線チャネル区間から暗号化された信号が受信されているかを判断する(S201)。その判断結果、暗号化された信号が受信されると受信された暗号化された信号から同期信号を検出する(S202)。

【0051】その後、段階S203で同期信号が検出されるのかを判断して、その判断結果、同期信号が検出されると、提供される解読キーにより任意の一定なランダムナンバーを生じる(S204)。続いて、前記発生したランダムナンバーにより前記受信された暗号化された信号を解読(Decrambling)した後(S205)、解読された信号、すなわち、PCMまたはパケットを提供される動作モードにより該モードを遂行した後、モード処理されたパケットを無線チャネル区間に伝

送する(S206)。ここで、該モードは、解読されたPCMをパケットに変換したり、または解読されたパケットをバイパスさせる動作を示す。

【0052】

【発明の効果】以上詳述したように、本発明による移動通信システムで音声／データの暗号化／復号化装置及びその方法は、無線チャネル区間から伝送されてきた信号をボコーディングまたはバイパスさせた後、ボコーディングまたはバイパスされた信号をランダムナンバーを利用してスクランプリングして有線チャネル区間に伝送して、有線チャネル区間から受信されるスクランプリングされた信号をデスクランプリングした後、ボコーディングまたはバイパスさせて無線チャネル区間に伝送することにより、システムボコダ間無線チャネル区間における保安性を画期的に維持させ盗聴を未然に防止することができる利点がある。また、今後、移動端末機とボコダとの間の無線チャネル区間まで拡張して全チャネル上で保安性を保障できる効果を有する。

【図面の簡単な説明】

【図1】 一般的な移動通信システムで移動加入者間の通話時、区間別伝送形態を示した図面である。

【図2】 一般的な移動通信システムでボコダバイパスされたパケット類型を示した図面であり、(a)はバイパスされた音声パケットのフォーマットを示した図面、(b)はバイパスされたデータパケットのフォーマットを示した図面である。

【図3】 従来技術による移動通信システムにおける動作モード別ボコーディング装置のブロック構成を示した図面である。

【図4】 本発明による移動通信システムにおける音声及びデータ暗号化／復号化装置のブロック構成を示した図面である。

【図5】 本発明による移動通信システムで音声及びデータ暗号化／復号化方法を示した流れ図である。

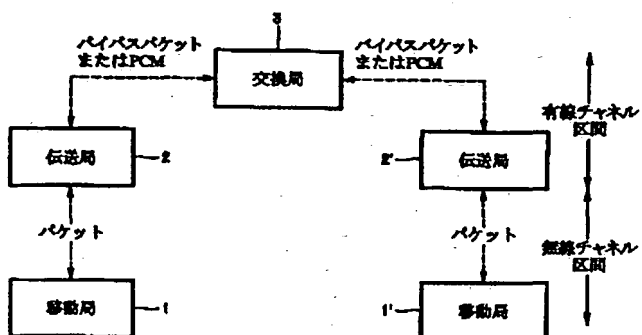
【図6】 本発明による移動通信システムで音声及びデータ暗号化／復号化方法を示した流れ図である。

【符号の説明】

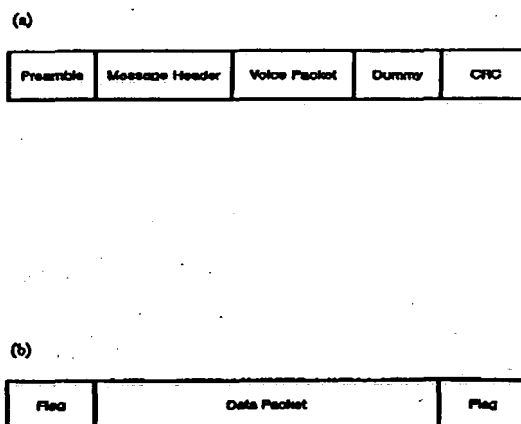
30 上位プロセッサ、40 ボコダ、41 動作モード処理部、42 制御部、43、48、50 スイッチング部、44 同期信号伝送部、45 暗号化シード部、46 ランダムナンバー発生部、47 スクランプリング部、49 同期信号検出部、51 デスクランプリング部。

(9)

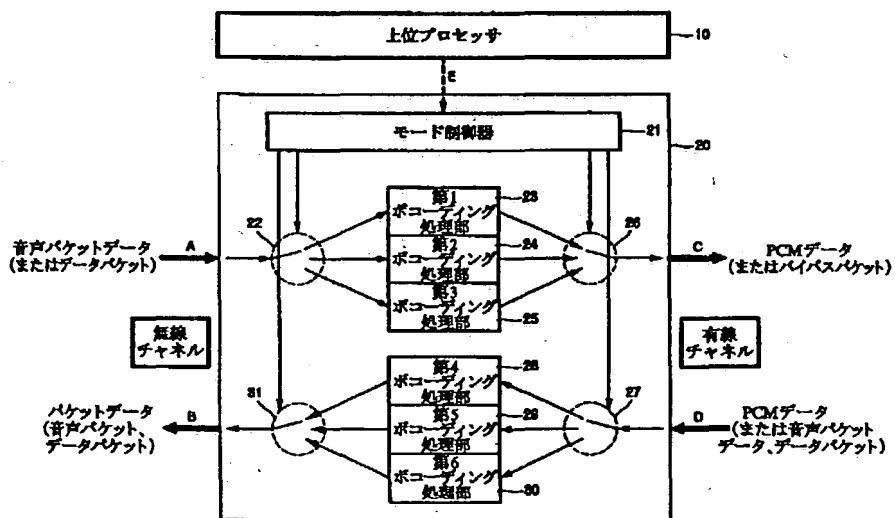
【図1】



【図2】

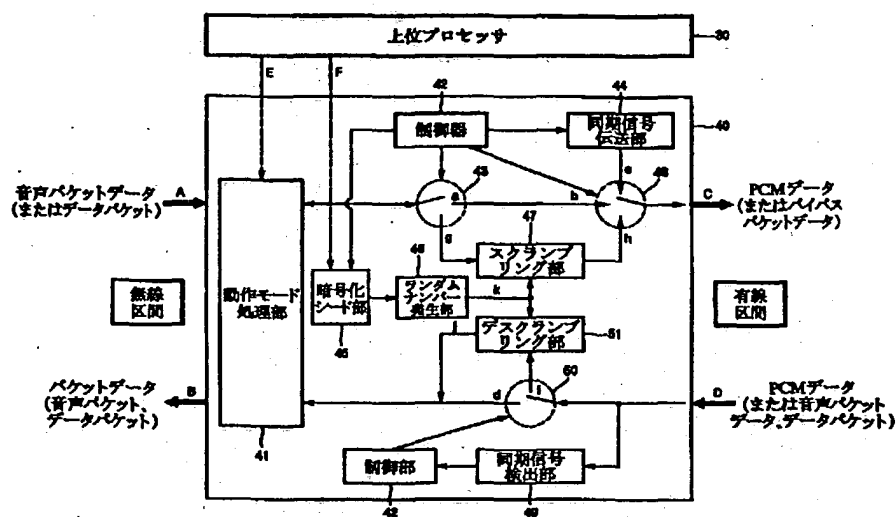


【図3】

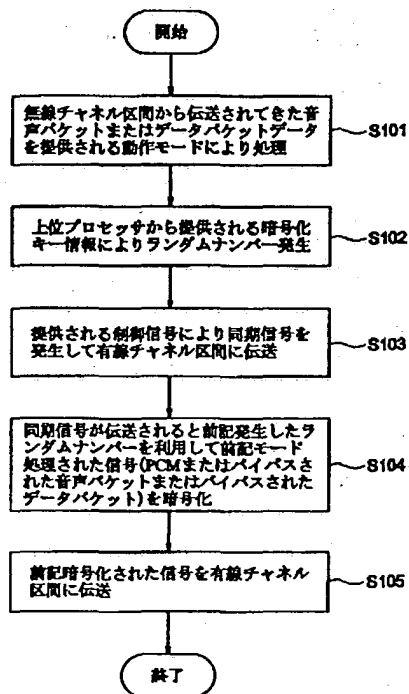


(10)

【図4】



【図5】



【図6】

